Heterogeneous Multi-Layer Adversarial Network Design for the IoT-Enabled Infrastructures

Juntao Chen, Corinne Touati, Quanyan Zhu

Heterogeneous Multi-Layer Adversarial Network Design for the IoT-Enabled Infrastructures

Abstract—**The emerging Internet of Things (IoT) applications that leverage ubiquitous connectivity and big data are facilitating the realization of smart everything initiatives. IoT-enabled infrastructures can be naturally divided into two layers including the existing infrastructure layer and the underlaid device network. The connectivity between different components in the infrastructure networks plays an important role in delivering real-time information and ensuring a high-level situational awareness. However, IoT-enabled infrastructures face cyber threats due to the wireless nature of communications. Therefore, maintaining the network connectivity in the presence of adversaries is a critical task for the infrastructure network operators. In this paper, we establish a three-player three-stage game-theoretic framework including two network operators and one attacker to capture the secure design of multi-layer infrastructure networks by allocating limited resources. We use subgame perfect Nash equilibrium (SPE) to characterize the strategies of players with sequential moves. In addition, we assess the efficiency of the equilibrium network by comparing with its team optimal solution counterparts in which two network operators can coordinate to design a secure network. We further design a scalable algorithm to construct the equilibrium secure IoT-enabled infrastructure networks. Finally, we use case studies on Internet of Battlefield Things (IoBT) to corroborate the obtained results.**

I. Introduction

The massive deployment of Internet of Things (IoT) technologies provides ubiquitous connectivity for heterogeneous machines and devices for data collection, information exchange and operational decision-making. Therefore, IoT is widely adopted in various application domains especially in infrastructures including smart grids, smart homes, intelligent transportation and smart cities [1].

With the current information and communication techniques (ICTs), an IoT-enabled infrastructure network has its own networking platform that is interoperable within the existing Internet infrastructure. Therefore, an integrated IoT-enabled infrastructure network can be naturally viewed as a *two-layer* network consisting of the infrastructure layer network and the device layer network. For instance, in the Internet of Battlefield Things (IoBT), the soldier networks equipped with wearable devices are integrated with the unmanned aerial vehicle (UAV) ad hoc networks to perform tasks. The connections in the two-layer IoT network architecture can be classified into two types: (i) the *interlinks* by which devices communicate between themselves as well as (ii) the *intralinks* by which devices communicate with the infrastructure.

The connectivity of an IoT-enabled infrastructure network plays an important role in information dissemination and real-time decision-making for mission-critical operations. Note that devices can communicate with each other or with infrastructures to maintain a global situational awareness of the infrastructure network. Furthermore, the IoT devices which are scarce of on-board computational resources can outsource heavy computations to the data centers through cloud computing infrastructure [2], [3]. IoT-enabled infrastructures are often vulnerable to attacks which can degrade the system performance, since most of the communications within the IoT networks are wireless in nature. For example, in IoBT networks, the communications between a soldier and a UAV relay node can be jammed by an attacker, and a soldier thus becomes isolated and loses information and awareness of the battlefield.

Therefore, to protect the infrastructures from adversarial behaviors, it is imperative to design secure and robust two-layer IoT networks that can maintain connectivity despite of link failures. Due to the heterogeneous and two-layer feature of the network, the design of the network is decentralized essentially. Specifically, the infrastructure network design involves two players who design their own subnetworks sequentially. As in IoBT networks, UAVs form their own relay networks, while a team of soldiers forms a network based on the knowledge of UAV locations to maintain the communications among soldiers and command and control stations. The objectives of these two network operators are to maintain the connectivity of the global network, while an attacker aims to disconnect the network at the minimum cost.

In this paper, we use a three-player three-stage game to capture the secure sequential IoT-enabled infrastructure network design. At the first stage, the network operator 1 creates links by anticipating the behavior of the network operator 2 and the adversary. At the second stage, the network operator 2 observes the links created by operator 1 and forms links to secure the network by anticipating the adversarial behaviors. Finally, the adversary observes the whole network created by the two operators and launches an attack targeting to disconnect the network. The two operators have aligned objectives to make the two-layer network connected. However, they have different costs or capabilities in forming communication links. For example, creating links between UAVs can be more expensive than links between soldiers as the distance between UAVs are much longer. In addition, the differences in network creativity and the ordering of the two network players can affect the outcome of the designed network.

We adopt subgame perfect Nash equilibrium (SPE) as the solution concept to the three-player sequential IoT-enabled infrastructure network design game. We first observe that the

SPE of the game results in a k-connected graph if the network remains connected at equilibrium. To understand the efficiency of the Nash equilibrium network, we use a centralized network design problem as a benchmark in which both operators coordinate and design an optimal secure network as a team. We further observe that the price of anarchy (PoA) is unbounded in general cases. However, when two subnetworks contain the same number of nodes and the unitary cost of creating intralinks is the same as that of forming interlinks of player 1, then the PoA is 2, which means that the maximum loss of efficiency through decentralized network design is 50%. Some counter-intuitive results are presented in Section III-C, e.g., the payoff of operator 1 is unique at SPE while operator 2's may vary. Finally, we use case studies on IoBT to illustrate the design principles of secure multi-layer infrastructure networks. With a higher threat level, the two network operators prefer more collaborations to secure the IoBT network.

Related Works: Security is a critical concern for IoT-enabled infrasturctures [3], [4]. Our approach is related to the recent advances in research on network formation [5], adversarial networks [6], [7], and network games [8], [9]. In particular, we address a heterogeneous multilayer network design problem and apply the framework to smart infrastructure networks.

The rest of the paper is organized as follows. Section II introduces the multi-layer IoT-enabled infrastructures framework and formulates the problem. Equilibrium infrastructure network analysis are presented in Section III. Section IV designs an algorithm to guide the secure solution network construction. Case studies on IoBT networks are provided in Section V, and Section VI concludes this paper.

II. Multi-Layer IoT-Enabled Infrastructure Model and Problem Formulation

We consider 2 infrastructure network operators and two sets of nodes $\mathcal{N}_1$ and $\mathcal{N}_2$, where nodes represent the devices and infrastructures in the IoT-enabled network. The first operator controls nodes in $\mathcal{N}_1$ and as such can create wireless communication links between those nodes as well as links connecting a node in $\mathcal{N}_1$ to one in $\mathcal{N}_2$. Similarly, the second operator controls nodes in $\mathcal{N}_2$ and can create links except those in $\mathcal{N}_1$. For convenience, we define the following notations:

- E_1 is the set of possible links between nodes of $\mathcal{N}_1$, that is $E_1 = \{e_1 = (n_a, n_b), n_a \in \mathcal{N}_1, n_b \in \mathcal{N}_1\}$.
- E_2 is the set of possible links between nodes of $\mathcal{N}_2$, that is $E_2 = \{e_1 = (n_a, n_b), n_a \in \mathcal{N}_1, n_b \in \mathcal{N}_2\}$.
- $E_{1,2}$ is the set of possible links between nodes of $\mathcal{N}_1$ and $\mathcal{N}_2$, that is $E_{1,2} = \{e_1 = (n_a, n_b), n_a \in \mathcal{N}_1, n_b \in \mathcal{N}_2\}$.

The adversarial IoT-enabled infrastructure network formation consists of three stages which are as follows.

- At round 1, operator 1 has the choice of creating a set of communication links in $E_1 \cup E_{1,2}$.
- At round 2, operator 2 can create a set of communication links in $E_2 \cup E_{1,2}$.
- At round 3, an adversary can remove a set of communication links, e.g., through jamming attacks, that have been created during the previous two rounds.

A network is a pair $(\mathcal{N}, \mathcal{E})$, with $\mathcal{N}$ a set of nodes and $\mathcal{E}$ a set of edges, or links between two nodes. At round 1, starting from an empty network $(\mathcal{N}, \emptyset)$, with $\mathcal{N} = \mathcal{N}_1 \cup \mathcal{N}_2$, operator 1 creates a set $\mathcal{E}_1 := \mathcal{E}_1^1 \cup \mathcal{E}_1^{1,2}$ of links and thus designs network $G_1 = (\mathcal{N}, \mathcal{E}_1)$ such that $\mathcal{E}_1$ is a subset of $E_1 \cup E_{1,2}$, the set of admissible links for operator 1, i.e., $\mathcal{E}_1^1 \subseteq E_1$ and $\mathcal{E}_1^{1,2} \subseteq E_{1,2}$. Then, at round 2, starting from network G_1, operator 2 creates a set $\mathcal{E}_2 := \mathcal{E}_2^2 \cup \mathcal{E}_2^{2,1}$ of links and thus designs network $G_2 = (\mathcal{N}, \mathcal{E}_1 \cup \mathcal{E}_2)$ such that $\mathcal{E}_2^2 \subseteq E_2$ and $\mathcal{E}_2^{2,1} \subseteq E_{1,2}$. Finally, at round 3, the adversary chooses a subset of the links $\mathcal{E}_A \subseteq \mathcal{E}_1 \cup \mathcal{E}_2$ that it removes from G_2, resulting in network $G_3 = (\mathcal{N}, \mathcal{E}_1 \cup \mathcal{E}_2 \backslash \mathcal{E}_A)$.

The goal of the operators is to construct a connected infrastructure network, that is a network where every node can be reached from any other through a sequence of links. Conversely, the role of the adversary is to obtain a network that is disconnected, and thus a node or a group of nodes becomes not accessible to the rest of the network. Let $\mathbb{1}_G$ be the indicator factor that equals 1 if network G is connected and 0 otherwise.

Both creating and removing links is costly. Let c_1 and c_2 be the unitary costs for creating a link for operators 1 and 2 in E_1 and E_2, respectively, and $c_{1,2}$ and $c_{2,1}$ be their corresponding unitary costs for creating a link in $E_{1,2}$. In addition, c_A is the cost of the adversary to remove a link. Then, the payoffs of operators 1, 2 and the adversary are, respectively,

$$
\begin{aligned}
U_1(\mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_A) &= \mathbb{1}_{(\mathcal{N}, \mathcal{E}_1 \cup \mathcal{E}_2 \backslash \mathcal{E}_A)} - c_1 |\mathcal{E}_1^1| - c_{1,2} |\mathcal{E}_1^{1,2}|, \\
U_2(\mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_A) &= \mathbb{1}_{(\mathcal{N}, \mathcal{E}_1 \cup \mathcal{E}_2 \backslash \mathcal{E}_A)} - c_2 |\mathcal{E}_2^2| - c_{2,1} |\mathcal{E}_2^{2,1}|, \\
U_A(\mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_A) &= 1 - \mathbb{1}_{(\mathcal{N}, \mathcal{E}_1 \cup \mathcal{E}_2 \backslash \mathcal{E}_A)} - c_A |\mathcal{E}_A|,
\end{aligned}
$$

where $|\cdot|$ denotes the cardinality of a set.

In this work, we are interested in seeking the subgame perfect Nash equilibrium (SPE) of the game, that is, we seek for optimal strategies of the three players as follows.

- Given network G_2, the adversary chooses the optimal set $\mathcal{E}_A^{\mathrm{MAX}}(\mathcal{E}_1, \mathcal{E}_2)$ that maximizes its utility $\mathcal{E}_A^{\mathrm{MAX}}(\mathcal{E}_1, \mathcal{E}_2) \in \arg\max_{\mathcal{F}} \{U_A(\mathcal{E}_1, \mathcal{E}_2, \mathcal{F})\}$.
- Given network G_1, operator 2 chooses the optimal set $\mathcal{E}_2^{\mathrm{MAX}}(\mathcal{E}_1)$ that maximizes its utility $\mathcal{E}_2^{\mathrm{MAX}}(\mathcal{E}_1) \in \arg\max_{\mathcal{F}} \{U_2(\mathcal{E}_1, \mathcal{F}, \mathcal{E}_A^{\mathrm{MAX}}(\mathcal{E}_1, \mathcal{F}))\}$.
- Operator 1 chooses the optimal set $\mathcal{E}_1^{\mathrm{MAX}}$ that maximizes its utility $\mathcal{E}_1^{\mathrm{MAX}} \in \arg\max_{\mathcal{F}} \{U_1(\mathcal{F}, \mathcal{E}_2^{\mathrm{MAX}}(\mathcal{F}), \mathcal{E}_A^{\mathrm{MAX}}(\mathcal{F}, \mathcal{E}_2^{\mathrm{MAX}}(\mathcal{F})))\}$.

By convention, the adversary attacks the network when $c_A|\mathcal{E}_A| = 1$ and $\mathbb{1}_{(\mathcal{N}, \mathcal{E}_1 \cup \mathcal{E}_2 \backslash \mathcal{E}_A)} = 0$ at SPE. In contrast, the operators will not secure the network if $c_1|\mathcal{E}_1^1| + c_{1,2}|\mathcal{E}_1^{1,2}| = 1$, $c_2|\mathcal{E}_2^2| + c_{2,1}|\mathcal{E}_2^{2,1}| = 1$, and $\mathbb{1}_{(\mathcal{N}, \mathcal{E}_1 \cup \mathcal{E}_2 \backslash \mathcal{E}_A)} = 1$.

Therefore, the SPE yields the equilibrium topology of the two-layer adversarial IoT-enabled infrastructure networks.

III. SPE Analysis and Analytical Results

In this section, we analyze the formulated three-player three-stage game in Section II with a focus on its SPE.

A. Backward Induction

To derive the SPE, we proceed by backward induction, that is we compute first the optimal strategy for the adversary, then operator 2 and finally operator 1.

Consider first the adversary strategy. We denote by p-connected a network $G=(\mathscr{N},\mathscr{E})$ that remains connected after the deletion of any p links and such that there exists a set $\mathscr{F}$ of $p+1$ links ($|\mathscr{F}|=p+1$) so that the network $(\mathscr{N},\mathscr{E}\backslash\mathscr{F})$ is disconnected. Any connected network $G=(\mathscr{N},\mathscr{E})$ is a p-connected network for some value of $1\leq p\leq|\mathscr{E}|$. By convention we say that a non-connected network is (-1)-connected. The value p is called the link connectivity of the network. We say that a network is p-resistant if it remains connected after the deletion of p links, that is, if it is m-connected for some $m\geq p$.

In the following, we let $k=\lfloor 1/c_A\rfloor$.

Lemma 1. *Let $\mathscr{E}_1$ and $\mathscr{E}_2$ be played by operator 1 and 2 respectively. Then, the adversary's optimal strategy $\mathscr{E}_A^{MAX}$ is:*

- *$\emptyset$ if $(\mathscr{N},\mathscr{E}_1\cup\mathscr{E}_2)$ is not connected,*
- *$\emptyset$ if $(\mathscr{N},\mathscr{E}_1\cup\mathscr{E}_2)$ is m-connected with $m\geq k$,*
- *any $\mathscr{F}$ such that $\mathbb{1}_{(\mathscr{N},\mathscr{E}_1\cup\mathscr{E}_2\backslash\mathscr{F})}=0$ and $|\mathscr{F}|=m+1$ if $(\mathscr{N},\mathscr{E}_1\cup\mathscr{E}_2)$ is m-connected with $m<k$.*

Proof. Note that since $1-\mathbb{1}_{(\mathscr{N},\mathscr{E}_1\cup\mathscr{E}_2)}\in\{0,1\}$ then the utility of the adversary is upper bounded by 1.

Further, if $\mathbb{1}_{(\mathscr{N},\mathscr{E}_1\cup\mathscr{E}_2)}=0$ (that is if $(\mathscr{N},\mathscr{E}_1\cup\mathscr{E}_2)$ is not connected), then $U_A(\mathscr{E}_1,\mathscr{E}_2,\mathscr{E}_A)=1$ if and only if $|\mathscr{E}_A|=0$, which is thus the (only) optimal strategy.

Assume now that $\mathbb{1}_{(\mathscr{N},\mathscr{E}_1\cup\mathscr{E}_2)}=1$. Note that $U_A(\mathscr{E}_1,\mathscr{E}_2,\emptyset)=1-\mathbb{1}_{(\mathscr{N},\mathscr{E}_1\cup\mathscr{E}_2)}=0$. Thus, the optimal strategy of the adversary is not the empty set if and only if there exists an $\mathscr{F}\neq\emptyset$ such that $\mathbb{1}_{(\mathscr{N},\mathscr{E}_1\cup\mathscr{E}_2\backslash\mathscr{F})}=0$ and $U_A(\mathscr{E}_1,\mathscr{E}_2,\mathscr{F})>0$.

Let m be the connectivity of network $(\mathscr{N},\mathscr{E}_1\cup\mathscr{E}_2)$. Let $\mathscr{F}$ be a non-empty set such that $(\mathscr{N},\mathscr{E}_1\cup\mathscr{E}_2\backslash\mathscr{F})$ is connected. Then, $U_A(\mathscr{E}_1,\mathscr{E}_2,\mathscr{F})=-c_A|\mathscr{F}|<0$. Thus this strategy is strictly dominated by the null strategy and therefore is not optimal. Reciprocally, let $\mathscr{F}$ be such that $(\mathscr{N},\mathscr{E}_1\cup\mathscr{E}_2\backslash\mathscr{F})$ is disconnected. Then $U_A(\mathscr{E}_1,\mathscr{E}_2,\mathscr{F})=1-c_A|\mathscr{F}|\leq 1-(m+1)c_A$. Thus, the null strategy is optimal if and only if $k\leq 1/c_A<m+1$, and a non-null strategy is optimal if and only if $m+1\leq 1/c_A<k+1$, that is if $m<k$. ☐

Thus, k can be interpreted as the maximum number of links that the adversary may attack at the SPE. In a similar vein, we can now detail the optimal strategy of operator 2:

Lemma 2. *Let $\mathscr{E}_1$ be played by operator 1. Then, the operator 2's optimal strategy $\mathscr{E}_2^{MAX}$ is:*

- *$\emptyset$ if $(\mathscr{N},\mathscr{E}_1)$ is k-connected;*
- *Otherwise, let F be the set of sets of $E_2\cup E_{1,2}$ such that for each element $\mathscr{F}$ of F, network $(\mathscr{N},\mathscr{E}_1\cup\mathscr{F})$ is k-connected. If F is not empty, we consider its element $\mathscr{F}$ that has the minimal cost, that is the set of links $\mathscr{F}=\mathscr{F}_2\cup\mathscr{F}_{2,1}$, where $\{\mathscr{F}_2,\mathscr{F}_{2,1}\}=\arg\min_{\mathscr{A}_2,\mathscr{A}_{2,1}}\{c_2|\mathscr{A}_2|+c_{2,1}|\mathscr{A}_{2,1}|$, s.t. $\mathscr{A}_2\subseteq E_2$, $\mathscr{A}_{2,1}\subseteq E_{1,2}\}$.*
  - *If $F=\emptyset$ or $c_2|\mathscr{F}_2|+c_{2,1}|\mathscr{F}_{2,1}|\geq 1$, then the optimal strategy of operator 2 is the null strategy and the resulting payoff is 0.*
  - *Otherwise (i.e. F is not empty and $c_2|\mathscr{F}_2|+c_{2,1}|\mathscr{F}_{2,1}|<1$), then the optimal payoff of operator 2 is $1-c_2|\mathscr{F}_2|-c_{2,1}|\mathscr{F}_{2,1}|$, and an optimal strategy is $\mathscr{F}$.*

This result leads us finally to the optimal strategy for operator 1:

Lemma 3. *Let $k=\lfloor 1/c_A\rfloor$. Let $\mathscr{G}$ be the set of k-connected networks. (Note that $\mathscr{G}$ is not empty iff $k+1\leq n-1$.) Any network of $\mathscr{G}$ can be written in the form $(\mathscr{N},\mathscr{E}_1^1\cup\mathscr{E}_1^{1,2}\cup\mathscr{E}_2^2\cup\mathscr{E}_2^{2,1})$ with $\mathscr{E}_1^1\subseteq E_1$, $\mathscr{E}_2^2\subseteq E_2$, $\mathscr{E}_1^{1,2}\subseteq E_{1,2}$ and $\mathscr{E}_2^{2,1}\subseteq E_{1,2}$. Now, let $\tilde{\mathscr{G}}\subseteq\mathscr{G}$ be the subset of k-connected networks that lead to positive utilities for operator 1 and 2, that is networks $\tilde{\mathscr{G}}=(\mathscr{N},\tilde{\mathscr{E}}_1^1\cup\tilde{\mathscr{E}}_2^2\cup\tilde{\mathscr{E}}_1^{1,2}\cup\tilde{\mathscr{E}}_2^{2,1})$ such that $c_1|\tilde{\mathscr{E}}_1^1|+c_{1,2}|\tilde{\mathscr{E}}_1^{1,2}|<1$ and $c_2|\tilde{\mathscr{E}}_2^2|+c_{2,1}|\tilde{\mathscr{E}}_2^{2,1}|<1$. Then, the optimal strategy of the first operator $\mathscr{E}_1^{MAX}$ is:*

- *$\emptyset$ if $\tilde{\mathscr{G}}=\emptyset$, and the associated payoff is 0.*
- *the elements of $\tilde{\mathscr{G}}$ that have the minimal value of $c_1|\tilde{\mathscr{E}}_1^1|+c_{1,2}|\tilde{\mathscr{E}}_1^{1,2}|$ otherwise.*

From Lemmas 1, 2, 3, we can finally deduce the SPE:

Lemma 4. *Let $\mathscr{E}_1$ be played by operator 1. Let $\mathscr{G}$ be the set of k-connected networks. Now, let $\tilde{\mathscr{G}}\subseteq\mathscr{G}$ be the subset of k-connected networks that lead to positive utilities for operator 1 and 2, that is networks $\tilde{\mathscr{G}}$ such that $c_1|\tilde{\mathscr{E}}_1^1|+c_{1,2}|\tilde{\mathscr{E}}_1^{1,2}|<1$ and $c_2|\tilde{\mathscr{E}}_2^2|+c_{2,1}|\tilde{\mathscr{E}}_2^{2,1}|<1$. Then:*

- *If $\tilde{\mathscr{G}}=\emptyset$, then the optimal strategy for operator 1 and 2 and adversary are emptysets and the resulting utilities are $U_1(\emptyset,\emptyset,\emptyset)=U_2(\emptyset,\emptyset,\emptyset)=0$ and $U_A(\emptyset,\emptyset,\emptyset)=1$.*
- *Otherwise, the optimal strategies of operator 1 are the elements of $\tilde{\mathscr{G}}$ that have minimal value of $c_1|\tilde{\mathscr{E}}_1^1|+c_{1,2}|\tilde{\mathscr{E}}_1^{1,2}|$. Then, if $\tilde{\mathscr{E}}_1^1\cup\tilde{\mathscr{E}}_1^{1,2}$ is the strategy of operator 1, the optimal strategies of operator 2 are the elements of $\tilde{\mathscr{G}}$ of the form $(\mathscr{N},\tilde{\mathscr{E}}_1^1\cup\tilde{\mathscr{E}}_1^{1,2}\cup\mathscr{E}_2^2\cup\mathscr{E}_2^{2,1})$ with $\mathscr{E}_2^2\subseteq E_2$ and $\mathscr{E}_2^{2,1}\subseteq E_{1,2}$ that minimizes $c_2|\mathscr{E}_2^2|+c_{2,1}|\mathscr{E}_2^{2,1}|$. Finally, the optimal strategy for the adversary is the null strategy leading to $U_A(\tilde{\mathscr{E}}_1^1\cup\tilde{\mathscr{E}}_1^{1,2},\mathscr{E}_2^2\cup\mathscr{E}_2^{2,1},\emptyset)=0$.*

In the following, we denote the SPE in the following format: $w=((\mathscr{E}_1^1,\mathscr{E}_1^{1,2}),(\mathscr{E}_2^2,\mathscr{E}_2^{2,1}),\mathscr{E})$ with $\mathscr{E}_1^1\cup\mathscr{E}_1^{1,2}$ the strategy of the first operator, $\mathscr{E}_2^2\cup\mathscr{E}_2^{2,1}$ the strategy of operator 2, and $\mathscr{E}$ the strategy of the adversary (with $\mathscr{E}\subseteq\mathscr{E}_1^1\cup\mathscr{E}_1^{1,2}\cup\mathscr{E}_2^2\cup\mathscr{E}_2^{2,1}$).

Suppose that $c_1\leq c_{1,2}$ and $c_2\leq c_{2,1}$. We can thus draw the following conclusion:

Lemma 5. *From Lemma 4, we have the following results: The only SPE is the null strategy for the three players, that is the SPE is $((\emptyset,\emptyset),(\emptyset,\emptyset),\emptyset)$ if any of the following condition is satisfied:*

- *$n_1+n_2-1<k+1$;*
- *$(k+1)\min(c_{1,2},c_{2,1})+\left\lfloor\frac{(n_1-1)(k+1)}{2}\right\rfloor c_1+\left\lfloor\frac{(n_2-1)(k+1)}{2}\right\rfloor c_2\geq 2$.*

In these cases, the SPE also corresponds to the optimal strategy for each of the 3 *players.*

Proof. We prove successively the two conditions:
(i) n_1+n_2-1 represents the maximal number of nodes that each node can connect to (i.e., the maximal degree). If this value is lower than $k+1$, then the adversary is able to disconnect any given network with at most k link removals.
(ii) Note that for the network to be k-resistant, each node should have a degree of (at least) $k+1$. Since there are n_1+n_2 nodes, then there are at least $\left\lceil \frac{(n_1+n_2)(k+1)}{2} \right\rceil$ links in the network. Further, $\mathscr{E}_1^{1,2} \cup \mathscr{E}_2^{2,1}$ should contain at least $k+1$ links. Since $c_1 \leq c_{1,2}$ and $c_2 \leq c_{2,1}$, then these links are the ones with maximal cost. Similarly, there are at least $\left\lfloor \frac{(n_1-1)(k+1)}{2} \right\rfloor$ links in $\mathscr{E}_1^1 \cup \mathscr{E}_1^{1,2}$ and at least $\left\lfloor \frac{(n_2-1)(k+1)}{2} \right\rfloor$ links in $\mathscr{E}_2^2 \cup \mathscr{E}_2^{2,1}$. □

In the following, we thus focus our attention in situations in which the conditions of Lemma 5 are not satisfied. Furthermore, we denote the set of SPE of the game by $\mathscr{L}^*$.

B. Efficiency of the Equilibria

From Lemma 4, at the SPE, the two operators sequentially form a network that is k-connected (if such network can be constructed so that they both receive a positive utility). In this section, we are interested in how different the costs are at the SPE and in a system where both operators can coordinate. We first present the definition of price of anarchy (PoA).

Definition 1 (Price of Anarchy)**.** *The PoA for the three-stage secure infrastructure network formation game is defined as*

$$PoA = \max_{w \in \mathscr{L}^*} \frac{C_{SPE}(w)}{C_{SO}},$$

where C_{SPE} and C_{SO} are the sum of costs for the operators at the SPE network and the sum of costs they would experience with coordination, respectively.

The following proposition shows that the individual costs as well as the global sum of costs can be arbitrarily different in the SPE and coordinated optimal infrastructure networks.

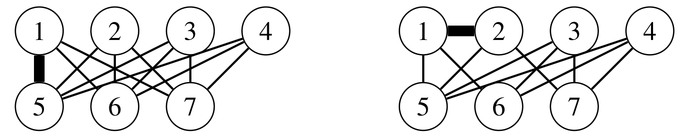
Proposition 1. *The PoA of the secure IoT-enabled infrastructure network formation game is unbounded.*

Proof. We consider a situation with $n_1 > 2$, $n_2 = 2$, $k = 1$, $c_1 = c_2 = \frac{1}{n_1^3}$, $c_{1,2} = \frac{1}{n_1^2}$ and $c_{2,1} = \frac{1}{3n_1}$.

An optimal joint strategy is to create all links of the form $(i, i+1)$ with $1 \leq i \leq n_1+1$ and link $(n_1+2, 1)$. As this construction forms a cycle of the n_1+n_2 nodes, then it is 1-connected. Further, it contains exactly $\left\lceil \frac{(n_1+n_2)(k+1)}{2} \right\rceil = n_1+n_2$ links, and among those $k+1 = 2$ are in $E_{1,2}$. It is therefore an optimal solution. Its cost is $C_{SO} = (n_1+n_2-2)c_1 + 2c_{1,2} = n_1c_1 + 2c_{1,2} = \frac{3}{n_1^2}$.

Next, we investigate the SPE of the game. The operator 1 plays the null strategy only if operator 2 can construct a 1-connected network at a cost lower than 1. We then consider the following strategy for operator 2 that consists in creating all links of the form (i, n_1+1) and (i, n_1+2) for all $1 \leq i \leq n_1$. This strategy has a cost of $C_{SPE} = 2n_1c_{2,1} = \frac{2}{3} < 1$, and the resulting network is 1-connected which can be shown by using Menger's theorem [10]. Indeed, for any nodes i and j, we can construct at least two disjoint paths. For instance, if i and j are both in $\mathscr{N}_1$, we consider the paths (both of length 2) $i; (i, n_1+1); n_1+1; (n_1+1, j); j$ and $i; (i, n_1+2); n_1+2; (n_1+2, j); j$. If $i \in \mathscr{N}_1$ and $j \in \mathscr{N}_2$, we consider the paths of length 1: $i; (i, j); j$ and the paths of length 3: $i; (i,k); k; (k,\ell); \ell; (\ell, j); j$ (with $k \in \mathscr{N}_1$, $k \neq i$ and $\ell \in \mathscr{N}_2$, $\ell \neq j$). Finally, if both i and j are in $\mathscr{N}_2$, then we consider the paths of length 2: $i; (i,1); 1; (1, j); j$ and $i; (i,2); 2; (2, j); j$. Note that this strategy is optimal for the second operator, since it creates $2n_1$ links in $E_{1,2}$.

The degradation of performance in terms of PoA for this example is finally $C_{SPE}/C_{SO} = \frac{2n_1^2}{9}$. □



(a) $\mathscr{E}_1^1 = \emptyset$ and $\mathscr{E}_1^{1,2} = \{(1,5)\}$. Then $|\mathscr{E}_2^{2,1}| = 11$.

(b) $\mathscr{E}_1^1 = \{(1,2)\}$ and $\mathscr{E}_1^{1,2} = \emptyset$. Then $|\mathscr{E}_2^{2,1}| = 10$.

Fig. 1: Non-unicity of the cost of operator 2. In both figures, the link created by operator 1 is represented by a bold line, while those of operator 2 are represented in plain thin lines.

C. Some Counter-Intuitive Results

In this section, we present some counter-intuitive results of the IoT-enabled infrastructure network formation game. The following Proposition 2 shows that for given system parameters, the SPE may not be unique. This, in terms of architecture is not surprising, since several topologies can lead to a k-connected network with minimal cost. More surprisingly, however is the fact that the SPE may not be unique in terms of costs.

Proposition 2 (Non-unicity of equilibrium cost)**.** *For given values of the parameters n_1, n_2, c_1, c_2, $c_{1,2}$, $c_{2,1}$ and c_A, the SPE may not be unique. More precisely, at the SPE, there is a unique payoff value associated to the operator* 1*, but there may be several payoff values of the operator* 2*.*

Proof. We show the result by providing an example with the property. Let parameters be $n_1 = 4$, $n_2 = 3$, $k = 2$, and $c_1 = c_2 = c_{1,2} = c_{2,1} = 0.09$.

From the value of c_2 and $c_{2,1}$, operator 1 knows that at the SPE, operator 2 builds at most 11 links. Since each node of $\mathscr{N}_1$ needs to have a degree of 3, if operator 1 builds no link, then operator 2 needs to build at least 12 links which is more than that it can bear. Thus operator 1 needs to build at least 1 link. Then, depending on the choice of the link created by operator 1, operator 2 needs to build either 10 or 11 links, as illustrated in Figure 1. □

In addition, the order of the operators creating their links has an impact on the payoffs of the players:

Proposition 3. *Consider an infrastructure network where the roles of the operators are symmetric, that is:*

$$n_1 = n_2,\ c_{1,2} = c_{2,1},\ c_1 = c_2.$$

Suppose that $n_1(k+1)c_{1,2} < 1$. Then at the SPE, the payoff of operator 1 is 1 while that of operator 2 is $1 - n_1(k+1)c_{1,2}$.

Proof. We consider the network $(\mathscr{N}, \mathscr{E})$ with $\mathscr{E} \subseteq E_{1,2}$. $\mathscr{E}$ is the set of links (i, j) with $1 \le i \le n_1$ and $n_1 + (i - \lfloor \frac{k}{2} \rfloor \mod n_2) \le j \le n_1 + (i + \lceil \frac{k}{2} \rceil \mod 2)$. Then, the network is k-connected and has exactly $\frac{(n_1+n_2)(k+1)}{2}$ links. □

IV. Secure Multi-Layer Network Construction

With the obtained SPE in Section III-A, the next critical step is to construct the secure infrastructure networks. In particular, we consider the scenario of $n_1 = n_2$. For clarity purposes, we further suppose that both n_1 and k are odd numbers.

To construct a k-resistant network, operators 1 and 2 need to jointly create a network that has at least $\left\lceil \frac{n(k+1)}{2} \right\rceil = n_1(k+1)$ links. This constitutes a lower bound on the number of links created (in a non-null strategy). Since k is odd, by using Menger's theorem [10], we propose a construction using a superposition of exactly $\frac{k+1}{2}$ independent Hamiltonian cycles. The algorithm for the network construction is depicted in Fig. 2, and for clarity, we decompose it into 4 stages as follows.

Stage 1*:* (Algorithm, line 1–12) In this stage, we determine the optimal values of $|\mathscr{E}_1^1|$ and $|\mathscr{E}_1^{1,2}|$.

Denote $e_1 = |\mathscr{E}_1^1 \cup \mathscr{E}_1^{1,2}|$. For a given e_1, note that the cost of operator 1 is minimized when $|\mathscr{E}_{1,2}|$ is minimized (since $c_1 \le c_{1,2}$). Further, for each node of $\mathscr{N}_1$ whose degree is d (with $d \le k+1$), operator 2 needs to create at least $k+1-d$ links in $E_{1,2}$. Note that any link of E_1 increases the degree of 2 nodes in $\mathscr{N}_1$ by 1, while any link of $E_{1,2}$ increases the degree of only 1 node in $\mathscr{N}_1$ by 1. Thus, each link created by operator 1 in E_1 allows to decrease $|\mathscr{E}_2^{2,1}|$ by 2, while each link created by operator 1 in $E_{1,2}$ allows to decrease $|\mathscr{E}_2^{2,1}|$ by only 1. Furthermore, for a given value of e_1, the cost of the second operator is minimized when $|\mathscr{E}_2^{2,1}|$ is minimized (since $c_2 \le c_{2,1}$, as long as the sum of degrees of nodes in $\mathscr{N}_1$ is less than $n_1(k+1) - (k+1)$ since $k+1$ links are required in $E_{1,2}$).

Thus, for a given value of e_1, both operators' costs are minimized when $|\mathscr{E}_1^{1,2}|$ is minimized, that is when operator 1 uses as many links between nodes of $\mathscr{N}_1$ as possible, as long as the sum of degrees of the nodes in $\mathscr{N}_1$ is less than $(n_1-1)(k+1)$. Thus, for a given e_1,

$$e_{11} = |\mathscr{E}_1^1| = \begin{cases} e_1 & \text{if } 2e_1 \le (n_1-1)(k+1), \\ (n_1-1)(k+1)/2 & \text{otherwise.} \end{cases}$$

Thus, operator 1 chooses the minimal value of e_1 and a set of links such that operator 2 can construct a k-resistant network with a cost lower than 1. Then, operator 1 computes its own resulting cost. If it is higher than 1, then no links are created and the SPE is $((\emptyset,\emptyset),(\emptyset,\emptyset),\emptyset)$. Otherwise, a network with e_1 links for operator 1 and $n_1(k+1) - e_1$ links for operator 2 is created.

Stage 2*:* (Algorithm, line 13–20) In this stage, we form m independent Hamiltonian cycles with $m = \left\lfloor \frac{e_{11}}{n_1-1} \right\rfloor$.

First, operator 1 creates links in E_1 in a similar manner as in Harary [11]. That is, it first creates links between nodes i and j such that $(|i-j| \mod n_1) = 1$, and then $(|i-j| \mod n_1) = 2$, etc. From [12], we know that a $2m$-Harary network contains exactly m independent Hamilton cycles of $\mathscr{N}_1$, that is cycles that go through all n_1 nodes and such that no link is used more than once. Further, [12] shows that there exists a construction such that links $(1;2)$, $(1;3)$, ..., $(1;m-1)$ all belong to different cycles. Thus, we remove those links from our construction and build all other links of the Harary network. We further construct $m(n_1-1)$ links in E_2 which are symmetric to as those in E_1. Hence, this stage creates $2m(n_1-1)$ links.

Further, for $1 \le i \le m$, by constructing two links, one between nodes 1 and n_1+i+1 and one between nodes n_1+1 and $i+1$, we form a Hamiltonian cycle between all nodes in $\mathscr{N}_1 \cup \mathscr{N}_2$. Note that all m different cycles use independent links. This further creates $2m$ links in $E_{1,2}$.

Stage 3*:* (Algorithm, line 21–27) In the case where $e_{11} > m(n_1-1)$, then operator 1 still needs to create $z = e_{11} - m(n_1-1)$ links in E_1.

In that case, we create an additional Hamiltonian cycle in the following manner. Starting from node 1, we consider the sequence $i_1; i_2; ...; i_{n_1}$ with $i_1 = 1$ and $i_{j+1} = (i_j + (n_1+1)/2) \mod n_1$. Since n_1 is odd, then for all $1 \le j, \ell \le n_1$ and $j \ne \ell$, we have $i_j \ne i_\ell$ or in other words the sequence $i_1; i_2; ...; i_{n_1}$ defines a permutation of indices $1, ..., n_1$. We then consider the following construction: for $j \le z$, we construct the links $(i_j; i_{j+1})$ and $(i_j + n_1; i_{j+1} + n_1)$ and for $z < j < n_1$, we construct the links $(i_j; i_{j+1} + n_1)$ and $(i_j + n_1; i_{j+1})$. This defines 2 sequences, and each one contains exactly n_1 nodes. By adding links $(1; n_1+1)$ and $((n_1+1)/2; n_1 + (n_1+1)/2)$, we create a full Hamiltonian cycle. Note that none of the links used previously have been created since $m < (k+1)/2$. This stage creates exactly either 0 link or $2n_1 = n$ links among which z links are in E_1, z links are in E_2, and $n - 2z$ links are in $E_{1,2}$.

Stage 4*:* (Algorithm, line 28–31) In total, either m or $m+1$ Hamiltonian cycles have been created and e_{11} links have been used. We thus create the remaining m_{12} Hamiltonian cycles with links exclusively in $E_{1,2}$ that have not been created in the previous stages. A possible solution for $k < n_1$ is as follows. For all t that satisfy $m < t < (k+1)/2$, we construct a Hamiltonian cycle following this pattern: for any $1 \le i \le n_1$, we create links $(i; (i+t \mod n_1) + n_1)$ and $((i+t) \mod n_1 + n_1; (i+1) \mod n_1)$ in the network.

The above 4 stages of construction yield an equilibrium two-layer secure infrastructure network.

V. Case Studies

In this section, we use case studies of IoBT to illustrate the optimal design principles of secure networks with heterogeneous components. In a battlefield scenario, the unmanned ground vehicles (UGV) and unmanned aerial vehicles (UAV) execute missions together. To enhance the information transmission quality and situational awareness of each agent in

Input: Parameters c_1, c_2, $c_{1,2}$, $c_{2,1}$, and odd n_1, k
Output: Network created by operator 1 and 2 at the SPE

Let $e_1 = 0$ // Number of links for operator 1 to build
Let $nb11 = (n_1 - 1)(k+1)/2$ // The maximal number of links in E_1
Compute $C_2(e_1) = n_1(k+1)c_{2,1}$ // Cost of operator 2
while $C_2(e_1) \geq 1$ // Increase e_1 until C_2 becomes lower than 1
do
  $e_1 = e_1 + 1$
  if $e_1 \leq nb11$ **then** $C_2(e_1) = C_2(e_1) - 2c_{2,1} + c_2$
  else $C_2(e_1) = C_2(e_1) - c_{2,1}$
Let $e_{12} = \max(0, e_1 - nb11)$; $e_{11} = e_1 - e_{12}$ // Number of links in $E_{1,2}$ and E_1 created by 1
Let $C_1(e_1) = e_{12}c_{1,2} + e_{11}c_1$ // Compute the resulting cost of operator 1
if $C_1(e_1) \geq 1$ // The SPE is $((\emptyset,\emptyset),(\emptyset,\emptyset),\emptyset)$.
then exit(0)
Set $m = \left\lfloor \frac{e_{11}}{n_1 - 1} \right\rfloor$ // Number of Hamiltonian cycles in E_1
for $i = 1$ *to* $m(n_1 - 1)$ // Create (n_1, m)-Harary network without links $(1,i)$ with $2 \leq i \leq m$
do
  Let $j, \ell \geq 0$, such that $i - 1 = \ell(n_1 - 1) + j$ and $j < n_1 - 1$
  $j = j + 2$; $\ell = \ell + 1$;
  Create links $(j; (j+\ell) \mod n_1)$ and $(j + n_1; ((j+\ell) \mod n_1) + n_1)$
for $i = 1$ *to* m // Create links in $E_{1,2}$ such that m Hamiltonian cycles are formed
do Create links $(1; n_1 + 1 + i)$ and $(n_1 + 1; 1 + i)$
Let $z = e_{11} - m(n_1 - 1)$ // Number of extra links in E_1
if $z > 0$ **then**
  $j = 1$
  for $\ell = 1$ *to* z **do** $p = (j + (n_1+1)/2) \mod n_1$; Create link (j, p) and $(j + n_1; p + n_1)$; Set $j = p$
  $j = 1$
  for $\ell = z + 1$ *to* $n_1 - 1$ **do** $p = (j + (n_1+1)/2) \mod n_1$; Create link $(j, p + n_1)$ and $(j + n_1; p)$; $j = p$
  Create link $(1; n_1 + 1)$ and $((n_1+1)/2; n_1 + (n_1+1)/2)$
Let $m_{12} = (k+1)/2 - m$; // Remaining Hamilton cycles in $E_{1,2}$
  if $z > 0$ **then** $m_{12} = m_{12} - 1$
for $\ell = 1$ *to* m_{12} **do**
  for $p = 1$ *to* n_1 **do** Create link $(p; (p + m + \ell + 1) \mod n_1 + n_1)$ and $(p + m + \ell + 1) \mod n_1 + n_1; (p+1) \mod n_1)$

Fig. 2: An algorithm to construct a possible solution network.

the battlefield, a secure and reliable communication network resistant to malicious attacks is critical.

In the following case studies, we consider $n_1 = 9$ UAVs and $n_2 = 9$ UGVs in the two-layer IoBT network. The normalized costs of creating different types of links are as follows: $c_1 = \frac{1}{30}$, $c_{1,2} = \frac{1}{20}$, $c_2 = \frac{1}{45}$ and $c_{2,1} = \frac{2}{45}$. In addition, the normalized unit cost of attack is $c_A = \frac{1}{3}$, and hence the attacker can compromise at most $k = 3$ links in the network. Based on Lemma 4, we obtain that, at SPE, the UAV network operator 1 creates 10 interlinks within its own network, and the UGV network operator 2 formulates 10 interlinks as well as 16 intralinks between two layers in the IoBT. Therefore, the equilibrium payoffs for operators 1 and 2 are $U_1^* = \frac{5}{6}$ and $U_2^* = \frac{1}{15}$, respectively. Note that the equilibrium IoBT network is a 3-connected network, and thus the attacker is incapable of disconnecting the system even with his best effort. By using the algorithm in Section IV, we construct the solution IoBT network resistant to 3 attacks as shown in Fig. 3.

We next investigate the impact of the number of attacks on the adversarial IoBT network formation. Specifically, the link creation costs are the same as those in the previous case study. We vary the attacker's capability k, and the obtained results are shown in Fig. 4. Fig. 4a illustrates the number of formed links of network operators 1 and 2 at the equilibrium IoBT configuration. When the attacker can compromise less than 2 links, the UGV network operator creates sufficient interlinks that connect UAVs and UGVs. Therefore, the utility of UAV network operator is 1. As the number of attacks increases, operator 1 begins to contribute to the network defense because operator 2 alone cannot secure the network with a positive payoff. For $2 \leq k < 7$, operator 1 allocates link resources only within the UAV network. In comparison, operator 2 creates

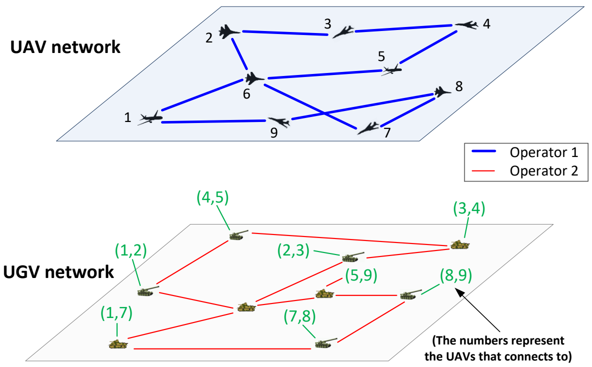
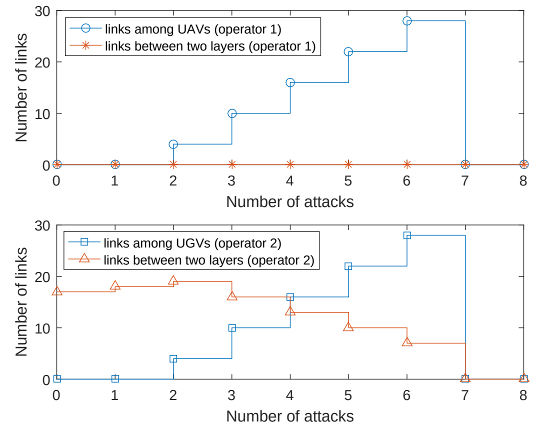
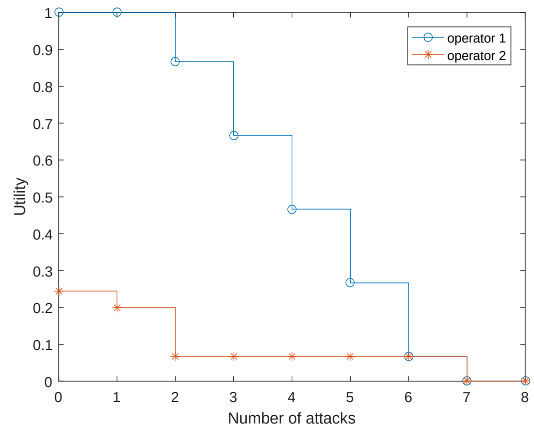


Fig. 3: The 3-connected equilibrium IoBT network.



(a) Number of links in the equilibrium network



(b) Equilibrium utility

Fig. 4: (a) shows the number of different types of links that operators 1 and 2 should create at the equilibrium IoBT network. (b) is the corresponding utility of two operators.

fewer intralinks and allocates more resources in its own UGV network as the cyber threats increase. In addition, when the number of attacks exceeds a certain level, i.e., $k \geq 7$ in this case, both network operators will cease to protect the network, and the corresponding SPE is a null strategy which satisfies the second condition in Lemma 5. Fig. 4b shows the utilities of two operators at the equilibrium IoBT network. The operator 1's payoff decreases as k grows. Interestingly, in the regime where the UAV network operator contributes to the secure IoBT network, i.e., $2 \leq k \leq 6$, the utility of UGV network operator remains the same which corresponds to the maximum effort that operator 2 can use. Based on this case study, we can conclude that higher threat levels induce more collaborations between two network operators.

VI. Conclusion

In this paper, we have investigated the multi-layer adversarial network design for the Internet of Things (IoT). To secure the heterogeneous IoT networks, we have formulated a three-player three-stage network formation game where two network operators aim to keep the network connected in the presence of attacks. The subgame perfect Nash equilibrium (SPE) of the game has been shown to be an empty set when the number of links that the attacker can compromise exceeds a threshold, or the link creations are too costly for the operators. The price of anarchy, i.e., the ratio of network formation costs between the SPE and team optimal strategies, of the game is unbounded. Furthermore, with a higher threat level, two network operators are more willing to collaborate to defend against attacks, since one operator alone cannot completely mitigate the threats with a limited amount of link allocation resources. Our future work would investigate the scenario in which network operators can protect the created links with some costs and study its SPE.

References

[1] Miorandi, Daniele, Sabrina Sicari, Francesco De Pellegrini, and Imrich Chlamtac. "Internet of things: Vision, applications and research challenges." Ad Hoc Networks 10, no. 7 (2012): 1497-1516.

[2] Kumar, Karthik, and Yung-Hsiang Lu. "Cloud computing for mobile users: Can offloading computation save energy?" Computer 43, no. 4 (2010): 51-56.

[3] J. Chen, and Q. Zhu. "Optimal Contract Design Under Asymmetric Information for Cloud-Enabled Internet of Controlled Things." in *Proceedings of International Conference on Decision and Game Theory for Security*, pp. 329-348. Springer International Publishing, 2016.

[4] M. J. Farooq, and Q. Zhu, "Secure and Reconfigurable Network Design for Critical Information Dissemination in the Internet of Battlefield Things (IoBT)," in *Proceedings of 15th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt), Telecom ParisTech*, Paris, France, 2017.

[5] Jackson, Matthew O. Social and economic networks. Princeton university press, 2010.

[6] M. Dziubiski, and S. Goyal. "Network design and defence." *Games and Economic Behavior* 79 (2013): 30-43.

[7] C. Bravard, L. Charroin, and C. Touati. "Optimal design and defense of networks under link attacks." *Journal of Mathematical Economics* 68 (2017): 62-79.

[8] J. Chen, and Q. Zhu. "Resilient and decentralized control of multi-level cooperative mobile networks to maintain connectivity under adversarial environment." in *Proceedings of the 55th Conference on Decision and Control (CDC)*, pp. 5183-5188. IEEE, 2016.

[9] J. Chen, and Q. Zhu. "Interdependent network formation games with an application to critical infrastructures." in *Proceedings of the American Control Conference (ACC)*, pp. 2870-2875. IEEE, 2016.

[10] Menger, Karl. "Zur allgemeinen kurventheorie." Fundamenta Mathematicae 10, no. 1 (1927): 96-115.

[11] F. Harary. The maximum connectivity of a graph. Proceedings of

the National Academy of Sciences of the United States of America, 48(7):1142, 1962.

[12] Jude Annie Cynthia, N. R. Swathi "Hamilton Decomposition of Harary Graphs", International Journal of Mathematics Trends and Technology (IJMTT). V34(2):59-63 June 2016.